1. OBJETIVO

A Política de Gerenciamento de Riscos e Controles Internos, abreviadamente "PGRCI", objetiva disseminar a cultura da gestão de riscos e o ambiente de controle em todos os níveis da Companhia, orientando os seus colaboradores quanto às ações que visam reduzir as exposições aos riscos (incertezas) com o objetivo de assegurar que os processos de identificação, análise, avaliação, priorização, tratamento, monitoramento, comunicação e gerenciamento dos riscos existentes, e/ou que possam se manifestar no futuro, observem as necessidades e melhores práticas estabelecidas pela Tupy. Além de contribuir para a tomada de decisões, maximizar as oportunidades de negócio através do atingimento dos objetivos estratégicos, e assegurar o cumprimento de leis, regulamentos e normativos internos e externos.

2. ABRANGÊNCIA

A PGRCI aplica-se a todas as áreas, macroprocessos e operações da Tupy S.A., subsidiárias e controladas que, direta ou indiretamente, participam do processo de Gerenciamento de Risco e Controles Internos, devendo ser conhecida e praticada por todo o quadro de colaboradores da Companhia.

Destina-se a qualquer área que utilize ou venha a utilizar as ferramentas disponibilizadas pela Gerência de Riscos e Controles Internos (GRCI), como suporte à condução dos seus processos para a redução da exposição aos riscos, internos ou externos, inerentes aos negócios da Tupy.

A Companhia possui política e normas específicas para tratar os riscos das operações financeiras, riscos de mercado e riscos de crédito.

3. REFERÊNCIAS

A PGRCI observará os seguintes documentos:

i. ABNT NBR IEC 31010 – Gestão de Riscos – Técnicas para Processo de Avaliação de Riscos
ii. ABNT ISO GUIA 73 – Gestão de Riscos – Vocabulário
iii. COSO's *Enterprise Risk Management – Integrated Framework*
iv. COSO's *Internal Control – Integrated Framework*
v. CEC – Código de Ética e Conduta Tupy
vi. DAI 001 – Regimento Auditoria Interna

vii. Estatuto Social da Companhia

viii. ISO 31.000:2018 – *Risk Management Guidelines*

ix. Política de Integridade da Tupy

x. Regulamento do Novo Mercado da B3

xi. *The Institute of Internal Auditors – Standards and Guidelines* (Instituto dos Auditores Internos - Padronização e Orientação)

4. DEFINIÇÕES

Administração: consideram-se administradores da Tupy os membros do Conselho de Administração e da Diretoria Estatutária.

Apetite ao Risco: grau de exposição que a Companhia está disposta a aceitar para atingir suas metas e objetivos, preservar e criar valor aos acionistas, estando diretamente relacionada à sua estratégia. O apetite ao risco é o nível aceitável de variação, considerando o atendimento de objetivos específicos da Companhia.

Avaliação de Riscos: processo integrado que envolve a identificação e a análise dos riscos aos quais a Companhia se encontra exposta.

Colaboradores: administradores, conselheiros, membros de comitês, empregados, estagiários, aprendizes e terceirizados.

Comitê de Auditoria e Riscos Estatutário (CAE): órgão sem poder deliberativo ou de gestão, com a atribuição de assessorar o Conselho de Administração no exercício de suas funções, com foco no acompanhamento e avaliação de riscos, de informações gerenciais, contábeis e de *Compliance*.

Comitê Executivo de Gerenciamento de Riscos e Controles Internos (CGRCI): Comitê vinculado à Diretoria Estatutária responsável pela tomada de decisão, de escolha e implementação de políticas alternativas de gerenciamento de riscos observados os parâmetros de apetite e tolerância aos riscos definidos pelo Conselho de Administração.

Conselho de Administração (CA): órgão colegiado a quem compete administrar a Companhia juntamente com a Diretoria Estatutária, observadas as disposições do Estatuto Social e da legislação em vigor.

Controle Interno: processo conduzido pelas estruturas de governança, administração e outros profissionais da Companhia, com o objetivo de proporcionar segurança razoável quanto à realização dos objetivos relacionados a operações, divulgação e conformidade, modificando os riscos do negócio, seja reduzindo a probabilidade de sua ocorrência, seja minimizando seus impactos negativos. Compreende o planejamento e todos os métodos e ações tomadas na

Companhia para salvaguardar seus ativos, verificar a exatidão e fidelidade dos dados contábeis, desenvolver a eficiência e segurança (patrimonial, física e ambiental) nas operações.

Diretoria Estatutária: órgão executivo colegiado de administração e representação, cabendo-lhe assegurar o funcionamento regular da Companhia em conformidade com a estratégia e orientação geral traçada pelo Conselho de Administração.

Dono do Controle (*Control Owner)*: responsável por executar e autoavaliar os controles internos, implementar e responder a planos de ação nos casos de detecção de deficiências.

Dono do Processo (*Process Owner*): responsável pelo processo na primeira linha, por garantir a execução das atividades de gerenciamento de riscos, revisar a classificação e monitorar a exposição a riscos. Avaliar os resultados da execução de controles e garantir a implementação de planos de ação.

Dono do Risco (*Risk Owner*): responsável direto pelo gerenciamento dos riscos associados às suas operações na primeira linha, por monitorar a execução dos controles e implementação de medidas corretivas para o seu devido tratamento. Apoiar na definição e implementação dos planos de ação necessários para remediação e/ou minimização destes.

Efeito: é um desvio em relação ao esperado – positivo e/ou negativo. Os efeitos podem ter diferentes aspectos (tais como metas financeiras, metas de desempenho, de saúde e segurança, ambientais etc.) e podem aplicar-se em diferentes níveis, tais como estratégico, organizacional, de projeto, de produto, de processo e outros.

Evento: incidente ou ocorrência, a partir de fontes internas ou externas à Companhia, capaz de afetar a realização dos objetivos.

Fatores de Risco: ocorrências específicas que por si só, ou combinadas com outras, podem gerar riscos ao negócio.

Gestão de Riscos: processo estruturado para identificação, análise, tratamento, monitoramento e comunicação dos riscos corporativos visando padronizar e orientar seu mapeamento e monitoramento, alinhando estratégia, processos, pessoas, tecnologia e conhecimentos, objetivando a preservação e criação de valores aos acionistas.

Impacto: resultado ou efeito de um evento, que a Companhia pode estar exposta em relação aos objetivos de negócio, antes e/ou depois da avaliação do respectivo risco, podendo ser de ordem tangível ou intangível de acordo com o apetite ao risco.

Incerteza: estado, mesmo que parcial, da deficiência das informações relacionadas a um evento e sua compreensão, ao seu conhecimento, à probabilidade de o evento acontecer e às suas consequências.

Key Performance Indicators* (KPI)*: ou Indicadores-Chave de Desempenho, têm por finalidade medir a etapa de um processo ou sistema, com acompanhamento periódico dos resultados

apresentados, auxiliando na avaliação e identificação de possíveis problemas ou dificuldades, considerando que diversas são as metas instituídas pela organização às atividades exercidas por seus colaboradores.

***Key Risk Indicators* (KRI):** ou Indicadores-Chave de Risco, são métricas utilizadas para determinar qual o potencial de exposição a um determinado risco, monitorando os níveis de risco de áreas específicas da Companhia, fornecendo informações significativas para o atingimento dos objetivos estratégicos e sinalizando a necessidade de ações a serem tomadas com maior tempestividade.

Modelo das Três Linhas: modelagem, instituída pelo IIA (*The Institute of Internal Auditors*) que enfatiza o papel das boas práticas de governança, no qual a estratégia deve estar alinhada à missão da Companhia, através do encorajamento de ações proativas, estabelecendo de forma clara e objetiva o gerenciamento de riscos e controles internos como responsabilidade da gestão.

Mapa de Riscos: instrumento não exaustivo onde são documentadas as principais exposições a riscos que necessitam ser avaliadas periodicamente e monitoradas pela Companhia, compreendendo todas suas áreas.

Matriz de Riscos: ferramenta de gerenciamento que permite visualizar a identificação de fatores de riscos, bem como sua combinação entre o impacto e a probabilidade, enfatizando aqueles que devem receber priorização junto com os respectivos planos de ações.

Plano Estratégico (PE): instrumento de caráter corporativo que consolida uma visão de quinze anos das estratégias e resultados pretendidos pela Companhia.

Política: conjunto de diretrizes da Companhia em relação a um tema relevante, aplicável a ela, suas subsidiárias e controladas que possuem quadro funcional. A Política norteia as ações em todos os níveis da Companhia.

Probabilidade: utilizada para referir-se à chance de algo acontecer, não importando se definida, medida ou determinada, ainda que objetiva ou subjetivamente, qualitativa ou quantitativamente, e se descrita utilizando-se termos gerais ou matemáticos.

Processo: conjunto de atividades estruturadas, inter-relacionadas e ordenadas internamente em áreas da Companhia, que utilizam entradas para entregar um resultado pretendido para atingir seus objetivos.

Risco: probabilidade de ocorrência de evento, de fontes internas e/ou externas, capaz de afetar negativamente a realização dos objetivos da Companhia, podendo abranger um ou mais aspectos, entre eles: reputacional, estratégico, financeiro, operacional, regulatório, de integridade, político, tecnológico, sistêmico, socioambiental, desvios de conduta e atos de natureza ilícita.

Riscos Estratégicos: riscos associados às decisões estratégicas da alta administração da Companhia que visam atingir seus objetivos de negócios, assegurando a capacidade ou habilidade da Tupy em proteger-se ou adaptar-se às mudanças do ambiente que ela esteja inserida.

Riscos Inerentes: risco presente antes do tratamento de riscos – ausência de qualquer ação que possa alterar o impacto ou probabilidade.

Riscos Residuais: risco remanescente, após o tratamento de riscos realizado pela Companhia.

***Stakeholders*:** são as partes interessadas, compreendendo todos os entes envolvidos com os negócios e operações da Companhia.

Tolerância ao Risco: a tolerância ao risco reflete a filosofia de gerenciamento de riscos da Companhia, correspondendo ao percentual de variações aceitáveis para realização do objetivo.

5. DISPOSIÇÕES GERAIS

5.1 DIRETRIZES

5.1.1 Gestão de Riscos e Controles Internos alinhada à Estratégia Corporativa

As diretrizes estabelecidas nesta PGRCI definem e caracterizam os macroprocessos de Gestão de Riscos Empresariais da Companhia, compreendendo:

- Fortalecimento da cultura do Gerenciamento de Riscos;
- Definição de papéis e responsabilidades;
- Padronização de conceitos;
- Disseminação de melhores práticas; e,
- Promoção dos objetivos da Companhia e da criação de valor aos acionistas.

As atividades de Gerenciamento de Riscos devem ser constantemente avaliadas, tomando como referência as práticas de Governança Corporativa definidas pelo COSO ERM: 2017 – Gerenciamento de Riscos Corporativos Integrado com estratégia e Performance e pela ISO 31000:2018 – *Risk Management Guidelines.*

A Tupy adota modelo de gestão de riscos baseado nos conceitos das Três Linhas instituída pelo IIA (*The Institute of Internal Auditors*), sendo:

- **Primeira linha:** representada por gestores das áreas de negócio e suporte, os quais devem assegurar a efetiva gestão de riscos dentro do escopo das suas responsabilidades organizacionais diretas.
- **Segunda linha:** refere-se às áreas de controle da Companhia, sendo responsável por apoiar, monitorar e questionar questões relacionadas a riscos e controles, bem como

suportar a 1ª Linha, fornecendo capacitação e apoio técnico no modelo de Gestão dos Riscos e Controles Internos.

- **Terceira linha:** atuando de forma independente e objetiva, tem como objetivo fornecer opiniões aos órgãos de Governança sobre o processo de gerenciamento de riscos e a efetividade dos Controles Internos.

1ª LINHA	2ª LINHA	3ª LINHA
PROCESS OWNER ▪ Garantir recursos aos *Risk Owners*, para a implementação das ações necessárias na mitigação de riscos; ▪ Revisar avaliações, informar ajustes da Matriz e apontar riscos não mapeados para GRCI; ▪ Reportar aos órgãos de governança status de planos de ação e contingências em desenvolvimento. ***RISK OWNER*** ▪ Avaliar e garantir que o risco está sendo mitigado e que os *Control Owners* estão exercendo suas atribuições; ▪ Implementar controles de prevenção e mitigação e designar *Control Owners;* ▪ Comunicar desvios aos *Process Owners.* ***CONTROL OWNER*** ▪ Executar controles e planos de ação. Comunicar desvios aos Risk Owners.	▪ Analisar, avaliar e monitorar os riscos identificados pela 1ª linha e sua efetividade; ▪ Auxiliar na identificação de riscos e no desenvolvimento de processos e controles; ▪ Fornecer orientações técnicas e suporte; ▪ Reportar tempestivamente aos órgãos de governança as informações relevantes relacionadas à gestão de riscos.	▪ Prestar avaliação e assessoria independente e objetiva sobre a adequação e eficácia da governança e do gerenciamento de riscos ao CAE (Comitê de Auditoria e Riscos Estatutários) e ao CA (Conselho de Administração) da adequação geral do ambiente.

Figura 01

5.1.2 Declaração de Apetite a Riscos

A Tupy S.A. promove a disseminação da cultura de integridade e altos padrões éticos, detendo forte consciência de risco, o que a estimula rever e desafiar as práticas existentes. Promove ambiente organizacional onde o desafio é uma parte natural das discussões e decisões sobre tomada de risco. Cumpre rigorosamente políticas, legislação, regulamentos e normas.

Estimula a inovação entre seus colaboradores através de investimentos em tecnologia e negócios em segmentos adequados à sua estratégia corporativa. A Companhia pugna pela sustentabilidade empresarial e socioambiental, a saúde e segurança de colaboradores e terceiros, a disciplina financeira, os padrões éticos e a segurança de ativos.

5.1.3 Boas Práticas de Governança Corporativa

Executar a gestão de riscos e controles internos com base nas melhores práticas de governança corporativa, de forma estruturada e adequada a seus objetivos.

5.1.4 Integração dos Processos

Promover o gerenciamento eficaz e eficiente de fatores de risco presentes em todas as unidades e áreas de negócio da Companhia.

5.2 PROCESSOS DA GESTÃO DE RISCOS

5.2.1 Estabelecimento do Contexto

Entendimento do negócio e seu contexto mercadológico contempla o ambiente externo (concorrência, geopolítica, economia, legislações, atos regulatórios, ambiental, etc.) e interno (cultura organizacional, planejamento estratégico, estrutura de capital, estabilidade financeira, etc.), formando a base de subsídios no processo de identificar, mensurar, tratar e priorizar riscos.

A declaração de Apetite ao Risco da Companhia é determinada a partir de parâmetros da escala de Impacto Financeiro em percentuais do EBITDA.

5.2.2 Identificação de Riscos

Os Riscos internos e externos aos quais a Companhia está exposta são periodicamente identificados, revisados e documentados em uma matriz de riscos. Busca-se nesta etapa também identificar riscos emergentes.

5.2.3 Análise, Avaliação, Priorização e Tratamento de Riscos

Avaliam-se os riscos inerentes – associados às operações/negócios/atividades – e os residuais – aqueles que permanecem ou que surgem após a inclusão de controles adicionais e/ou ajustes dos controles existentes – bem como a probabilidade e o impacto a fim de direcionar a decisão sobre a priorização de riscos. Cada risco avaliado possui um dono e o resultado da combinação entre Probabilidade e Impacto, recebe uma nota final de “A”, “B” ou “C”, conforme figura 2.

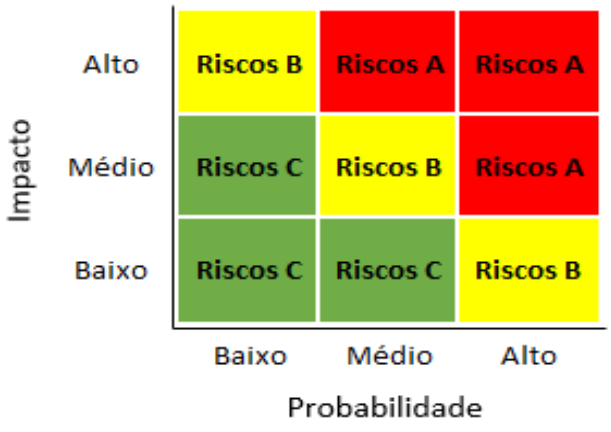

Figura 02

Os riscos são tratados da seguinte forma:

- **Riscos "A":** Representam riscos prioritários que demandam ação imediata para se buscar a eliminação/mitigação do fator de origem de riscos, com a elaboração de planos de ação e/ou implementação de controles internos;
- **Riscos "B":** Riscos de criticidade média que exigem atenção, cujo foco deve ser o de definir níveis aceitáveis de perda por eventos e limites de competência que evitem que o nível de impacto seja majorado ao longo do tempo, com a elaboração de planos de ação e/ou implementação de controles internos;
- **Riscos "C":** Riscos sujeitos à implementação de controles internos consistentes com seus níveis de criticidade.

Após conduzir uma avaliação dos riscos a administração determina como responderá aos riscos. As alternativas para tratamentos dos riscos classificam-se da seguinte forma:

a. Eliminar as atividades que geram o evento de risco;
b. Diminuir a probabilidade de ocorrência e/ou a magnitude de impacto do evento de risco;
c. Transferir ou compartilhar parte do evento de risco; e
d. Aceitar o evento de risco.

5.2.4 Comunicação

Implantação de processos contínuos e interativos a todas as partes interessadas, que permitam fornecer os resultados de todas as etapas do processo de gestão de riscos, para auxiliar no entendimento dos riscos e da eficácia dos planos de ação.

5.2.5 Monitoramento

O monitoramento tem como objetivo avaliar a efetividade do processo de Gestão de Riscos, por meio de atividades gerenciais contínuas e/ou avaliações independentes. Consiste na verificação, supervisão e observação crítica executadas de forma contínua, a fim de identificar mudanças no nível de desempenho requerido ou esperado. A área de GRCI é responsável por monitorar e reportar o andamento dos planos de ação para os riscos elencados.

5.3 CONTROLES INTERNOS

5.3.1 Finalidade

Os Controles Internos da Companhia devem permitir à Administração monitorar os processos operacionais e financeiros, assim como os riscos de desconformidade e descontinuidade, de acordo com as políticas, normas e os limites estabelecidos pelo Conselho de Administração, propiciando sustentabilidade e perenidade para os negócios da Companhia.

As atividades de controles devem ser constantemente avaliadas, tomando como referência as boas práticas de Governança Corporativa estabelecidas pelos padrões e metodologia do *Commitee of Sponsoring Organization of Treadway Commission* – COSO e do *Control Objectives for Information and related Technology* (CobiT).

5.3.2 Objetivos

Os controles internos da Tupy têm como objetivo:

- Proporcionar a eficiência, a eficácia e a efetividade operacional, mediante execução ordenada, ética e econômica das operações;
- Assegurar a conformidade com as leis e regulamentos aplicáveis, incluindo normas, políticas, programas, planos e procedimentos;
- Salvaguardar e proteger bens, ativos e recursos contra desperdício, perda, mau uso, dano, utilização não autorizada ou apropriação indevida.

O Gerenciamento dos controles internos da Companhia utiliza os seguintes conceitos e estruturas:

- **CSA - *Control Self Assessment*:** processo de autoavaliação realizado pelas áreas de negócio para avaliar o desenho e a implantação dos controles internos, e se estão sendo executados em conformidade com seus objetivos;
- **ToE - *Test of Effectiveness*:** processo de testes de efetividade de controle interno utilizado para atestar que os controles são executados adequadamente pelas áreas de negócio, permitindo identificar eventuais deficiências;
- ***Sign-Off*:** processo utilizado pela administração da Companhia para efetuar a aprovação dos resultados das avaliações dos controles internos.

6. ATRIBUIÇÕES E RESPONSABILIDADES

6.1 CONSELHO DE ADMINISTRAÇÃO - CA

a. Aprovar diretrizes para o processo integrado de gerenciamento de riscos e controles internos da Tupy (metodologia, processos, sistemas, política, padrões e mecanismos de reporte, dentre outros);
b. Deliberar o apetite a risco em consonância com os planos estratégicos;
c. Aprovar os riscos estratégicos priorizados e seus respectivos planos de resposta e contingência;
d. Aprovar a PGRCI e suas revisões;
e. Aprovar a metodologia da Matriz de Riscos;
f. Avaliar periodicamente o portfólio de riscos estratégicos, o Mapa de Riscos e a execução dos Planos de Ação mitigatórios;
g. Garantir e supervisionar que sejam disponibilizados os recursos necessários ao pleno funcionamento da estrutura de gestão de riscos e do sistema de controles internos.

6.2 COMITÊ DE AUDITORIA E RISCOS ESTATUTÁRIO - CAE

a. Assessorar o Conselho de Administração na aprovação dos riscos estratégicos a serem priorizados e de seus respectivos planos de mitigação e contingência, bem como das modificações na avaliação de criticidade dos riscos, do apetite e tolerância a risco e da definição de diretrizes e políticas para o processo de gerenciamento de riscos integrados aos controles internos;
b. Assessorar o Conselho de Administração na análise das avaliações anuais e periódicas das auditorias independentes relacionadas aos processos de gerenciamento de riscos e controles internos;
c. Avaliar o processo e estrutura de gerenciamento de riscos e a efetividade dos controles existentes para garantir o tratamento dos riscos e o seu monitoramento;
d. Monitorar a existência de critérios para avaliação, mapeamento e classificação de riscos bem como a existência de controles para o seu monitoramento;
e. Acompanhar os resultados, planos de ações mitigatórias e de contingências dos processos de gerenciamento de riscos e de controles internos e reportar eventuais recomendações ao Conselho de Administração;
f. Supervisionar a evolução do grau de eficiência dos controles internos;

g. Monitorar a qualidade e a integridade dos mecanismos de gerenciamento de riscos e de controles internos.

6.3 DIRETORIA ESTATUTÁRIA

a. Avaliar e propor atualizações/alterações na PGRCI;
b. Garantir a aplicação da PGRCI em toda a Companhia, incorporando as práticas de gestão de riscos e controles internos ao processo decisório;
c. Identificar e validar os riscos das respectivas áreas de acordo com o apetite e tolerância a riscos;
d. Aprovar o Plano Anual da área de GRCI;
e. Revisar e aprovar o portfólio de riscos estratégicos;
f. Definir os donos dos riscos e donos de processo;
g. Avaliar os planos de ação sugeridos pelos donos dos riscos e aprovar eventuais postergações de prazos;
h. Definir expectativas sobre integridade, valores éticos, transparência e responsabilidades para o cumprimento dos controles internos;
i. Monitorar as avaliações de controles e planos de ações realizadas pelas áreas de negócio no processo de CSA, solicitando resposta tempestiva para as deficiências identificadas;
j. Indicar a necessidade de avaliações independentes do processo de gerenciamento de riscos e controles internos (agentes internos ou externos), de modo a assegurar sua eficácia;
k. Garantir o desenvolvimento contínuo dos profissionais atuantes em gerenciamento de riscos e controles internos da Companhia;
l. Assegurar autonomia aos agentes de controles internos da Companhia no exercício de suas atividades, garantindo o acesso a documentos, sistemas de informação e pessoas, e demais elementos necessários ao exercício de suas atividades;
m. Assegurar o alinhamento entre o Planejamento Estratégico e GRCI, visando o adequado tratamento dos riscos;
n. Assegurar os recursos necessários para a execução dos planos de ação de mitigação de riscos;
o. Validar os relatórios de controles internos emitidos pela Auditoria Interna sobre a efetividade dos controles;
p. Propor a aprovação da Matriz de Riscos da Companhia.

6.4 COMITÊ EXECUTIVO DE GERENCIAMENTO DE RISCOS E CONTROLES INTERNOS – CGRCI

a. Analisar e propor estratégias para os processos de gerenciamento de riscos e controles internos;
b. Analisar e apresentar pontos de melhoria no processo de gerenciamento de riscos e controles internos (metodologia, processos, sistemas, política, padrões e mecanismos de reporte, dentre outros);
c. Subsidiar a Diretoria na elaboração de propostas para a deliberação do apetite a risco pelo Conselho de Administração;
d. Avaliar e deliberar para a diretoria Estatutária o plano de trabalho de gerenciamento de riscos;
e. Avaliar os níveis de alçada de riscos, os quais definem as responsabilidades para sua aprovação e tratamento;
f. Identificar e analisar os controles internos nas áreas, visando avaliar sua eficácia, suficiência e aplicabilidade na mitigação dos riscos aos quais estão relacionados;
g. Identificar, construir e acompanhar os indicadores-chave de risco (KRI's - *Key Risk Indicators*) e acompanhar os indicadores-chave de performance (KPIs – *Key Performance Indicators*), buscando sempre utilizar ambos os conjuntos de indicadores como ferramentas de gestão de riscos e controles internos;
h. Avaliar a matriz de riscos e de controles internos, mantendo-as sempre atualizadas e visando sempre aprimoramentos constantes;
i. Supervisionar o mapeamento e avaliação dos riscos que podem comprometer o atingimento dos objetivos estratégicos da Companhia;
j. Elaborar e supervisionar método de priorização de temas e macroprocessos para gerenciamento de riscos e implementação dos controles internos da gestão;
k. Acompanhar mensalmente o resultado das ações mitigatórias e dos indicadores de riscos propostos para o tratamento dos riscos estratégicos priorizados, propondo diretrizes ou ações visando o enquadramento, a adequação e a mitigação dos riscos que eventualmente apresentarem níveis acima do tolerado;
l. Acompanhar periodicamente o resultado das avaliações dos sistemas de controles internos dos processos;
m. Analisar e recomendar sobre portfólio e planos de tratamento de riscos estratégicos sempre que houver atualizações;
n. Analisar e propor priorização de riscos estratégicos;

o. Analisar e recomendar a elaboração de planos de tratamento resultantes das avaliações dos sistemas dos controles internos dos processos;
p. Monitorar as recomendações e orientações deliberadas pelo próprio Comitê;
q. Avaliar e recomendar recursos necessários para a execução dos processos de gerenciamento de riscos e controles internos;
r. Zelar pelo cumprimento da PGRCI;
s. Posicionar sobre as atividades do Comitê Executivo, quando demandado pela Diretoria Estatutária, Comitê de Auditoria Estatutário e Conselho de Administração, elaborando, quando demandado, manifestação técnica relativa aos temas de sua competência.

6.5 VICE-PRESIDÊNCIA DE FINANÇAS E ADMINISTRAÇÃO

a. Constituir e aplicar ferramentas e mecanismos de gestão de riscos e controles internos adequados à aplicação desta Política;
b. Mensurar e avaliar a qualidade dos mecanismos;
c. Elaborar e submeter proposta de revisão desta Política, sempre que necessário;
d. Promover sistemática de debates e discussões desdobradas em seus fóruns de atuação e junto às gerências, de modo a assegurar a eficácia do gerenciamento e do monitoramento dos riscos;
e. Coordenar o Comitê Executivo de Gerenciamento de Riscos e Controles Internos (CGRCI);
f. Zelar pelo cumprimento da PGRCI;
g. Definir as respostas aos riscos (evitar, mitigar, compartilhar ou aceitar).

6.6 PRIMEIRA LINHA

6.6.1 Donos de Processo (*Process Owner*)

a. Apoiar o Dono do Risco em suas atribuições e atividades;
b. Suportar ao Dono de Risco os meios para a implementação das ações necessárias para mitigação dos riscos, garantindo o envolvimento e as adequadas entregas das áreas intervenientes;
c. Recomendar ajustes na Matriz de Riscos quando julgar necessário e garantir o registro dos riscos nas hipóteses em que eles não se enquadrem nos temas já existentes na matriz vigente, envolvendo eventuais mudanças significativas na probabilidade e/ou impacto do risco ou em qualquer outra característica e, caso identifique, riscos não mapeados;

d. Revisar a criticidade do risco (impacto *versus* probabilidade), considerando alterações em ações mitigatórias existentes, conclusão dos planos de ação e de contingência;
e. Certificar (*Sign off*), anualmente ou sob demanda, que os riscos relacionados aos processos sob sua responsabilidade estão adequadamente identificados, avaliados e registrados no sistema de gestão de riscos;
f. Efetuar, quando demandado, reportes aos órgãos de governança sobre o desenvolvimento dos planos de ação para a mitigação dos riscos e dos planos de contingências;
g. Participar das reuniões periódicas promovidas pela área de GRCI ou órgãos de governança, quando convocado.

6.6.2 Donos do Risco (*Risk Owner)*

a. Tratar os riscos que estão sob sua responsabilidade, identificando, avaliando, tratando, prevenindo e monitorando os riscos de forma integrada;
b. Desenvolver indicadores para monitorar a variação e os resultados do risco sob sua responsabilidade;
c. Garantir a implantação de ações necessárias para a mitigação dos riscos, juntamente com o envolvimento de outras áreas, implementando e executando, de forma proativa, quaisquer ações de mitigação ou de eliminação que julgar necessário, de transferência ou de compartilhamento ou de rejeição dos riscos de nível inaceitável;
d. Elaborar reportes sistemáticos para apresentar à área de GRCI e ao Comitê Executivo de Riscos e Controles Internos, o acompanhamento do risco sob sua responsabilidade;
e. Acompanhar e reportar ao Dono do Processo, para sua validação, os resultados e as análises críticas dos indicadores de riscos, das ações mitigatórias, bem como a atualização do impacto financeiro, conforme calendário pré-determinado pela área de GRCI;
f. Subsidiar o Dono do Processo e à área de GRCI de eventuais mudanças significativas na probabilidade e/ou impacto do risco ou em qualquer outra característica e, caso identifique, riscos não mapeados;
g. Informar tempestivamente ao Dono do Processo da área e à GRCI acerca de eventos que possam alterar a avaliação do Risco, bem como avaliar temas aplicáveis ao Mapa de Riscos nas diferentes geografias;
h. Avaliar continuamente a aplicabilidade dos temas de riscos da Matriz de Riscos às atividades sob sua responsabilidade;

i. Propor para o Dono do Processo, e este para a área de GRCI o tratamento dos Riscos sob sua responsabilidade e assegurar a elaboração e execução de Planos de Ação;
j. Comunicar à área de GRCI, eventos que possam impactar a execução dos controles pré-estabelecidos, assim como a necessidade de criação de novos controles para mitigação dos riscos;
k. Atuar nos pontos críticos criando e executando os planos de remediações necessários;
l. Implementar controles efetivos de prevenção e de mitigação, garantir adequada definição e execução dos planos de ação e estabelecer ações corretivas para a melhoria contínua da gestão de riscos;
m. Assegurar a conformidade com regulamentações externas, políticas e normas internas;
n. Assegurar, para riscos no nível de monitoramento contínuo, a efetividade dos controles e a tempestividade dos planos de ação;
o. Quando julgar necessário, solicitar suporte adicional ao dono do processo para evoluir no tratamento preventivo dos riscos sob sua responsabilidade;
p. Atender as diretrizes, padrões técnicos e de gestão mínimos definidos pelas 2ª Linha;
q. Realizar a revisão técnica do risco, dos seus fatores, da criticidade do risco (impacto *versus* probabilidade), considerando alterações em ações mitigatórias existentes, conclusão dos planos de ação e de contingência;
r. Participar das reuniões periódicas promovidas pela área de GRCI ou órgãos de governança, quando convocado.

6.6.3 Donos de Controle (*Control Owner)*[1]

a. Disponibilizar dados e informações ao Dono do Risco para revisão técnica do risco, dos seus fatores, da criticidade (impacto *versus* probabilidade) e da resposta, considerando alterações em ações mitigatórias existentes e propostas e plano de contingência;
b. Executar os controles de prevenção e mitigação que lhe forem atribuídos, zelando sempre pela acuracidade e tempestividade da informação e segurança do processo, em conformidade com a legislação aplicável, políticas e normas internas, e buscar a correção dos controles, em caso de detecção de alguma deficiência;
c. Realizar a autoavaliação de controles (CSA), respeitando a frequência definida no controle, dando suporte e condições para a execução da avaliação dos sistemas de controles internos relacionados aos processos sob sua responsabilidade;

[1] Donos de controle, eventualmente também podem estar mapeados em funções de segunda linha.

d. Elaborar e executar planos de ação para controles que julgue deficientes ou que necessitem implementação;
e. Executar e responder tempestivamente os planos de ação relacionados aos controles.

6.7 SEGUNDA LINHA

6.7.1 **Gestão de Riscos e Controles Internos - GRCI**

a. Apoiar e promover continuamente a cultura de Gestão de Riscos e Controles Internos na Companhia, disseminando conceitos, conhecimentos e boas práticas em todos os níveis de colaboradores;
b. Propor e revisar diretrizes para os processos de Gerenciamento de Riscos e Controles Internos (metodologia, processos, sistemas, política, portfólio de riscos, padrões e mecanismos de reporte, dentre outros), atualizando periodicamente os procedimentos decorrentes desta Política;
c. Desenvolver, conduzir e aplicar metodologia para identificação, avaliação e monitoramento dos riscos e controles internos junto às áreas da Companhia;
d. Propor, para aprovação das instâncias superiores, a Matriz de Riscos da Companhia e relatórios ou análises decorrentes dela;
e. Elaborar, revisar e atualizar o portfólio de riscos sempre que houver atualizações no mapa de riscos da Companhia ou quando eventos relevantes ocorrerem, reportando à Diretoria, ao Comitê Executivo de Gerenciamento de Riscos e Controles Internos e ao Comitê de Auditoria e Riscos Estatutário;
f. Auxiliar na definição dos Donos dos Processos, Donos dos Riscos, Donos do Controle e demais agentes de controles internos, auxiliando-os na definição dos indicadores de riscos, ações de tratamento e planos de contingências;
g. Acompanhar mudanças na criticidade dos riscos estratégicos e reportá-las ao Comitê Executivo de Gerenciamento de Riscos e à Diretoria Estatutária;
h. Elaborar e revisar periodicamente o plano de trabalho de gerenciamento de riscos;
i. Suportar a divulgação externa de informações oficiais referentes à gestão de riscos de negócio;
j. Acompanhar a elaboração e execução dos planos de ação necessários para mitigação dos riscos, em conjunto com as demais áreas da Companhia;
k. Documentar e avaliar o desenho dos processos de negócio quanto à exposição de riscos, identificando oportunidades de melhoria e necessidade de implantar controles internos;

l. Suportar a 1ª Linha, fornecendo capacitação e apoio técnico no modelo de Gestão dos Riscos da Companhia;
m. Manter os controles internos atualizados e aderentes aos processos da Companhia, apoiando as áreas envolvidas no processo de CSA e planos de remediação e o processo de Sign Off;
n. Atuar em conjunto com a Diretoria, Comitê Executivo de Gerenciamento de Riscos e Controles Internos, Comitê de Auditoria e Riscos Estatutário e Conselho de Administração, na discussão sobre a definição do apetite e tolerância a risco da Companhia;
o. Monitorar o alinhamento entre o Planejamento Estratégico e o Gerenciamento de Riscos e Controle Interno, visando o adequado tratamento dos riscos;
p. Reportar mensalmente os resultados à Diretoria e ao Comitê Executivo de Gerenciamento de Riscos e Controles Internos, e a cada bimestre ao Comitê de Auditoria e Riscos Estatutário e ao Conselho de Administração;
q. Garantir que as recomendações relacionadas a riscos e controles internos, feitas pelas Auditorias Interna e Externa, órgãos fiscalizadores e controladores externos, sejam incorporadas ao mapeamento dos processos e aos planos de tratamento.

6.7.2 Outras Áreas

Outras áreas da Companhia – além de GRCI, Segurança do Trabalho, Meio Ambiente e Compliance – também atuam como 2ª Linha dos respectivos riscos potenciais. Essas áreas têm como atribuições:

a. Conhecer, disseminar e atuar dentro das diretrizes corporativas de Gestão de Riscos da Tupy;
b. Definir metodologias, padrões técnicos, tecnológicos e de gestão mínimos, indicadores de riscos a serem adotados pela 1ª Linha;
c. Atuar como apoio à 1ª Linha, por meio de avaliação dos conceitos adotados, verificação se os riscos possuem controles mapeados e se as barreiras implementadas são as melhores em cada situação relacionada a riscos relevantes;
d. Apoiar na identificação dos riscos, necessidade de implementação de controles adicionais e não conformidades dos controles existentes e emitir recomendações, dar suporte técnico na implementação do modelo e de padrões de gestão e de prevenção de riscos e de ativos;

e. Traçar os planos de ação de mitigação de riscos corporativos de sua competência, reportando à GRCI o tratamento e os planos de ações de mitigação de riscos;
f. Avaliar a aplicação dos padrões e indicadores pelas áreas operacionais, comerciais, de projetos, de suporte e administrativas (1ª Linha), com independência e transparência;
g. Pautar potenciais riscos relevantes em fóruns aplicáveis, caso sejam necessárias deliberações de ações preventivas que demandem suporte adicional.
h. Estabelecer, manter, promover e avaliar as práticas de negócio eficientes e controles internos adequados e eficazes;
i. Documentar os controles internos implementados nas respectivas áreas da Companhia;
j. Apresentar à Gerência de GRCI a documentação dos controles internos implantados nas respectivas áreas de sua competência.

6.8 TERCEIRA LINHA

6.8.1 Auditoria Interna

a. Certificar a efetividade dos controles implementados para mitigação de riscos (ToE);
b. Alinhar o plano de auditoria aos riscos do negócio;
c. Reportar os resultados das avaliações de controle interno e o acompanhamento das tratativas das deficiências dos controles internos.

7. RESPONSABILIZAÇÕES

A inobservância das responsabilidades/atribuições definidas na presente Política deverá ser examinada pela área de GRCI e submetidas para avaliação do Comitê Executivo de Gerenciamento de Riscos e Controles Internos (CGRCI), o qual submeterá à Diretoria Estatutária para as providências a serem adotadas para fins de apuração de responsabilizações à luz do que prevê o Código de Ética e Conduta da Companhia.

Colaboradores de qualquer nível ou área da Companhia, inclusive *stakeholders*, que observarem quaisquer desvios às diretrizes desta Política poderão relatar o fato aos Canais de Denúncias.

8. EXCEÇÕES

As situações de exceção não previstas na presente Política devem ser submetidas à área de GRCI para avaliação e posterior reporte ao Comitê Executivo de Gerenciamento de Riscos e Controles Internos (CGRCI).

9. DISPOSIÇÕES FINAIS

O conteúdo da presente Política poderá ser alterado apenas mediante aprovação do Conselho de Administração, sempre que o referido órgão da administração entender necessário ou em decorrência de alterações regulatórias.

Vigência: a partir 24 de junho de 2022.

3ª versão: 06/2022

Responsáveis pelo documento:

Responsável	**Área**
Elaboração	Gestão de Riscos e Controles Internos
Revisão	Diretoria Estatutária e Comitê de Auditoria e Riscos Estatutário
Aprovação	Conselho de Administração